TOP TEN TIPS FOR CLOUD SECURITY

If you're thinking of moving any IT function to a cloud-based service, it is critical that you make sure that both the service and the vendor are fit for purpose. But short of a costly and time-consuming full audit of each vendor, what can you do to ensure your data is safe and the service will be there when you need it?

01 **Confidentiality** – Ask questions regarding the controls in place for physical security, staff access to customer data, penetration testing and incident handling. If the vendor is going to be storing data for an extended period of time, ask about the way the data is encrypted, and more importantly how the encryption keys are managed. It's no good encrypting something if the bad guys can access the keys!

02 **Integrity** – Quiz the vendor about development processes, quality assurance and testing. Some smaller, more agile vendors have been known to rush through new features in order to please customers, with unexpected results. However, as with confidentiality, integrity becomes more serious when the vendor is being asked to store critical data for an extended period. It is a good idea to ask about the number of copies of the data being held and the number of data centres it is being held in.

03 **Availability** – Data and systems are no good to you if they aren't there when you need them. Most vendors will give you an availability SLA but it is still a good idea to ask about the infrastructure being used to support your service.

04 **Legality** – Including governments, military and certain finance companies, there is no law that prohibits the use of cloud-based services for scanning or storing data. External email and web traffic is already being sent across the public internet and, given the way the internet works, companies have no control over the countries through which it may be transported or where it may be stored.

05 **Cost** – Cloud-based services can at first glance appear to be more costly than the equivalent on-premise solution. To really work out the equivalent costs, you need to carry out a total cost of ownership exercise over the expected lifespan. Avoid using vendor-specific TCO calculators. Instead, create a spreadsheet which includes the purchase costs of all elements of the solution, the implementation costs and then the running costs. Make sure that you take acquisition costs into consideration, an on-premise solution will need to be disposed of and replaced every 3-5 years whereas a cloud-based solution will be constantly upgraded by the vendor.

Symantec

TOP TEN TIPS FOR CLOUD SECURITY

CONTINUED

06 **Service Level Agreements** – SLAs are a vitally important component of a hosted solution. In fact it could be argued that they are what you are paying your money for. With an on-premise solution you are responsible for keeping it running, tuning it to achieve optimum performance, monitoring it and being there to fix it when it goes wrong. With a cloud-based solution you are paying for the business results. The trick is to look behind the headlines. For example, if a company offers a 100% virus detection SLA you could first check whether that only covers known viruses or if it covers all viruses. Then check to see what happens if the SLA is broken and how you claim. Lack of an SLA shouldn't stop you using an online storage vendor, you just need to compare the risks against those of keeping it yourself in your own data centre.

07 **Administration** – A great cloud-based service should be more than just a virtual version of your on-premise solution. It should ideally be much simpler and require less resource to manage. When you are choosing your cloud-based solution, have a look at the user interface. If you are required to define spam rules and alter sensitivities then the vendor is passing the buck.

08 **Support** – What happens if something critical goes wrong with your email delivery, archive retrieval or web access? Do you need to pay extra for better levels of service and if so, how much will it cost to get the level you need? Some vendors who primarily offer services to small businesses and home users may want you to access support through forums, some vendors may want to charge you per incident and some may have extra costs for out-of-hours telephone support.

09 **Ease of implementation** – Make sure that you confirm whether or not your cloud-based solution requires any on-premise components. Many solutions have connectors for tasks such as single sign on, active directory synchronisation or end-user access to an archive.

10 **Certification and accreditation** – The most meaningful certification for a cloud- based vendor is ISO 27001, which covers information security management systems. ISO certification is time consuming, expensive and challenging for a vendor to obtain and so is normally a good indicator of quality. But make sure you check which parts of the vendor's business are included in the scope of the certification.

In general, a vendor's overall track record, financial stability and existing customer base are always good measures of reliability and quality. If your vendor has been providing cloud-based, multi-tenanted email security and archiving to highly security-conscious customers such as banks, pharmaceutical companies or even governments, then you can be pretty sure as to the quality of the service that they are providing.

Symantec